AO 106 (Rev. 04/10) Application for a Search Warrant (requesting AUSA Roberta Benjamin)

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
ZTE N9132 CELLULAR PHONE
Serial No. 3258572706BB

Case No. 17-659-m

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Search Warrant Attachment A incorporated herein

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Search Warrant Attachment B incorporated herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 2251	online enticement of a minor

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: ___________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[signature]
Applicant's signature

DANIEL J. JOHNS, SPECIAL AGENT
Printed name and title

Sworn to before me and signed in my presence.

Date: May 15, 2017

[signature: Lynne A. Sitarski]
Judge's signature

City and state: Philadelphia, Pennsylvania

Hon. Lynne A. Sitarski , U.S. Magistrate Judge
Printed name and title

17-659-M

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Daniel J. Johns, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI for nine years, and am currently assigned to the Philadelphia Division's Violent Crimes Against Children Squad. While employed by the FBI, I have investigated federal criminal violations related to counterterrorism, Internet fraud, computer intrusions, and the FBI's Innocent Images National Initiative, which investigates matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, training at the Innocent Images Unit of the FBI, various conferences involving Innocent Images and Crimes Against Children, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for a ZTE N9132, serial number 3258572706BB (Subject Phone), currently in the possession of the FBI and belonging to ANDREW ENGDAHL, listed in Attachment A, for the items specified in Attachment B hereto.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe

are necessary to establish probable cause to believe that evidence of violations of Title 18 U.S.C. Sections 2251, 2252 and 2252A is located in the Subject Phone.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of Title 18 U.S.C. Section 2251 which makes it a crime to persuade, induce entice or coerce a minor to engage sexually explicit conduct for the purpose of producing any visual depiction of such conduct, and any attempts to do so.

6. In summary, the following facts establish that there is probable cause to believe ANDREW ENGHADL utilized the Subject Phone to persuade, induce, entice or coerce a minor to engage in sexual explicit conduct for the purpose of producing a visual depiction and evidence is located in FBI custody at 600 Arch Street, Philadelphia, PA 19106.

LEGAL AUTHORITY

7. Title 18 U.S.C. § 2251 prohibits Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

DEFINITIONS

8. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See Title 18 U.S.C. § 2256(5)).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. § 2256(2)).

e. "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the

Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. § 2510(15)).

j. "Hash Value" is a mathematical value generated by applying an algorithm to a computer file, that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, a hash value is generally considered to be a unique signature or fingerprint for a file.

BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES AND THE INTERNET

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Cell phones and more advanced devices known as "smart phones" function the same as computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.

d. GPS, or Global Positioning System, devices can be portable devices used to obtain directions to destinations or show roads and directions in a given area. GPS devices can store the route an individual traveled. GPS devices have been used by individuals to obtain directions when they travel to meet a minor for sexual purposes.

e. Child pornographers can convert photographs into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

f. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

h. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, Sky Drive or One Drive, and Dropbox among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device, such as a cell phone or “smart phone”, with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer devices in most cases.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR

10. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage.

g. Recent studies have shown that those who collect child pornography are more likely to be "contact offenders" with children. In a study published in the Journal of Abnormal Psychology, Vol. 15, No. 3, pp. 610-615, by Seto, Cantor, and Blanchard, titled Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia, the authors concluded an interest in child pornography is a strong indicator of pedophilia. In December, 2010, Seto, Hanson, & Babchishin, published an article entitled Contact Sexual Offending by Men With Online Sexual Offenses, in Sexual Abuse: A Journal of Research and Treatment. This article was a meta-analysis of a number of studies of possessors of child pornography. This was a meta-analysis of 24 studies of possessors of child pornography. In the studies that relied only upon subsequent arrests and/or convictions, the number of contact offenses with children ran from 4.6% to 13.3%. In the three studies in which the subjects were subject to polygraph examinations, the percentages ranged from 32.3% to 84.5%, with the middle study finding 55.3%. In the remaining three studies which relied only upon self-reporting, the numbers ranged from 32.8% to 57.4%. Each of the last three studies was unique. In Neutze, Seto, Schaefer, Mundt, & Beier (in press at this time), the subjects were in Germany. They had sought counseling on their own and were not referred by the criminal justice system. In the venue where the study was conducted, therapists were not legally required to report the admissions of their subjects (36.5%). In Quayle & Taylor (2003), the number of subjects was sample small (23) and had established good rapport with the therapists (47.8%). Finally, in Coward, Gabriel, Schuler, and Prentky (2009), the subjects reported anonymously (32.8%). In performing their statistical analysis of these studies, Seto, Hanson, & Babchishin concluded that more than 50% of those convicted of possession only admitted to at least one contact offense, when one relied on more than an arrest or conviction for a new offense. Most recently, Bourke, Fragomeli, Detar, Sullivan, Meyle, and O'Riordan published an article in March 2014 in the Journal of Sexual Aggression entitled "The Use of the Tactical Polygraph with Sex Offenders." They found that 57.5% of those under investigation solely for possession, receipt, or distribution who were polygraphed at or near the time of the execution of a search warrant admitted to hands-on offenses against children. (They disclosed 170 previously unknown victims.)

BACKGROUND OF THE INVESTIGATION

11. The FBI received a complaint from the mother of a seven year old child (M1). M1 stated that her seven year old child was contacted on Facebook by a man who gave his name as Andrew Engdahl. Engdahl told the child that he lived in Pennsylvania and sent an image of his face. M1 was very concerned about the conversation because Engdahl had said inappropriate things to her daughter like asking how she played with her baby dolls or what she was wearing when in bed. M1 used her daughters account to communicate with Engdahl. While M1 used the account, Engdahl asked for a full body pic. Based on my training and experience in investigating cases involving images of child pornography, a "full body pic" means a nude picture of the minor.

12. On May 8, 2017 FBI Special Agents interviewed Engdahl at his residence, 200

West Broad Street, Quakertown, PA 18951, Apartment 300. Engdahl consented to a search of the Subject Phone.

13. A search of the subject phone yielded images of what appeared to be a minor female's vagina. The image depicts a lascivious exhibition of the genitals and/or public area of the minor. Engdahl stated the images depicted a minor female ("V1"). Engdahl knew V1 from his job at the local gas station. Engdahl believed V1 was 14, 15 or 16 years old. Engdahl received the images from V1 via Facebook Meessenger. Engdahl stated he never had sexual intercourse with V1. Engdahl informed Agents he had intended to delete these images, but had not yet done so.

14. Additionally located during the search of the phone were several images that appeared to be of minor female children with their vaginas exposed, again depicting a lascivious exhibition of the genitals and/or public area of the minor. When questioned about these images, Engdahl stated that the children were eighteen years or older. Based on my training and experience in investigating and viewing images of child pornography, the pictures appear to be of children under the age of 18. Engdahl stated he seeks out nude beach websites and most photographs on his phone are from these sites. Engdahl stated that he is a Wiccan and has a spiritual belief to be free and be who you are. Endahl sleeps nude because of these beliefs. Engdahl also believes that 18 as an age of consent can be too limiting. If a child is sixteen and wants to have sex, then they are going to have sex. Engdahl stated that if his daughter wanted to have sex, he would make sure it was safe and that she did not do something she didn't want to do.

16. Engdahl has a website on his "favorites" within the Subject Phone browser. Engdahl told agents that the website "has a lot of child porn on it." The website doesn't have full nudity, but there are many tabs to click on. One of the tabs was "young" which appeared to be under the age of 18. Engdahl assumed it meant 18.

17. Based upon Engdahl's aforementioned intent to delete the child pornography images, agents seized the Subject Phone, which is currently located in FBI custody at 600 Arch Street, Philadelphia, PA 19106.

SEARCH METHODOLOGY TO BE EMPLOYED

18. To search for electronic data contained in computer, phone, or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

19. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the

file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

20. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

CONCLUSION

21. Based upon the information above I respectfully submit that there is probable cause to believe that violations of Title 18 U.S.C. Sections 2251 have been committed and that evidence of those violations is located on the Subject Phone, currently in FBI custody at 600 Arch Street, Philadelphia, PA 19106. This evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property, which is or has been used as the means of committing the foregoing offenses.

22. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

DANIEL J. JOHNS
Special Agent, Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
BEFORE ME THIS 15th DAY
OF MAY, 2017.

Lynne A. Sitarski

HONORABLE LYNNE A. SITARSKI
United States Magistrate Judge

ATTACHMENT A

ZTE N9132 Cellular phone

This is a black cellular phone with a maroon strip on the side and "ZTE"affixed on the rear. The serial number for this cellular phone is 3258572706BB.

MEID
DEC
MEID
HEX
S/N

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of United States Code Title 18, Section 2251, Section 2422, Enticement of a Minor (with underlying Pennsylvania violations of Statutory Sexual Assault (18 Pa.C.S.A. § 3122.1), Involuntary Deviate Sexual Intercourse (18 Pa.C.S.A. § 3123), Indecent Assault (18 Pa.C.S.A. § 3126), Unlawful Contact with a Minor (18 Pa.C.S.A. § 6318)) and involve ANDREW ENGDAHL, including:

a. Images of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256; communications with minors seeking to entice them to send images of sexually explicit conduct, in violation of 18 U.S.C. §§ 2251 and 2422; or to engage in sexual activity in violation of 18 U.S.C. § 2422.

b. Any data on the cellular telephone used to identify this cellular telephone on a network including, but not limited to:

i. IMSI: The **International Mobile Subscriber Identity** (IMSI) which is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.

ii. IMEI: The **International Mobile Station Equipment Identity** (IMEI) is a number, usually unique used to identify 3G mobile phones (i.e., GSM, UMTS and LTE).

iii. MEID: A **mobile equipment identifier** (MEID) is a globally unique number identifying a physical piece of CDMA mobile station equipment.

iv. ESN: An **Electronic Serial Number** (ESN) a 32-bit control number used for cell phone activation in wireless carrier networks.

c. Any data on the cellular telephone which identifies the subscriber and/or the subscriber's account.

d. Any contacts on the cellular telephone, including, but not limited to, names, telephone numbers, contact information, and notes

e. Any Simple Message Service (SMS) messages or MMS (multi-media service) messages, commonly referred to as "text messages", on the cellular telephone, relating to an effort to induce or coerce a minor to engage in sexual activity;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in Paragraph 1a were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, text messages, and browsing history;

3. Evidence of the location of the phone during times in contact with minors.

4. Evidence of photos, images, or videos pertaining to minor children that are evidence of a sexual interest in children.

5. Evidence of mobile applications utilized to communicate with minors, whether through public postings or private messages.

6. Evidence of mobile applications utilized in the production, receipt, or distribution of child pornography.-